# PERLINDUNGAN HUKUM TERHADAP KERAHASIAAN DATA PRIBADI NASABAH DALAM PENYELENGGARAAN SISTEM ELEKTRONIK DI SEKTOR JASA KEUANGAN

**Alfrets Florentino Supit[1], Maryano[2], Gatut Hendro Triwidodo[3]**
[1,2.3] Program Magister Ilmu Hukum, Pascasarjana Universitas Jayabaya,Jakarta,Indonesia

e-mail:2024010261049@pascajayabaya.ac.id

CORPUS JURIS
JURNAL ILMU HUKUM

**E-ISSN : 3109-9173**
**CORPUS JURIS: Jurnal Ilmu Hukum**
https://manggalajournal.org/index.php/corpusjuris/

Vol. 2, No. 2 Agustus 2026

Page: 353-369

**DOI:**
https://doi.org/10.62335/corpusjuris.v2i2.2944

**Article History:**
Received:
04-08-2026

Revised:

04-08-2026

Accepted:

23-08-2026

***Abstract*** *: In its efforts to protect personal data, the government has established various legal instruments governing personal data protection, the operation of electronic systems, and the governance of the financial services sector, as embodied in Law Number 27 of 2022 concerning Personal Data Protection. Furthermore, as Electronic System Providers, business entities in the financial services sector are obligated to comply with requirements regarding the reliability, security, and protection of electronic systems, as stipulated in Government Regulation Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions. Nevertheless, the existing regulations require further analysis to determine whether they provide adequate legal protection for the personal data of customers held by Electronic System Providers in the financial services sector. The research addresses the following issues: the legal framework governing customer personal data protection within electronic systems in Indonesia's financial services sector, and the legal protection of the confidentiality of customer personal data disclosed to third parties during the operation of such electronic systems. The study employs the theories of legal protection and privacy. The research method used is a normative juridical legal approach which is strengthened by interviews. This research uses a statutory research approach, a case approach, an analytical approach and a conceptual approach, which in principle comes from primary legal materials consisting of laws and case studies, secondary legal materials consisting of books, research results, articles and tertiary legal materials from libraries, articles and websites. Legal material analysis techniques use grammatical interpretation techniques. The research findings indicate that the legal regulations governing the protection of customer personal data within electronic systems in Indonesia's financial services sector have essentially established a framework that limits the collection, storage, use, and transfer of personal data to third parties; furthermore, legal protection for the confidentiality of customer data transferred to third parties is provided through both preventive and repressive instruments. The*

*study recommends strengthening the regulation and supervision of the transfer and processing of customer personal data by third parties—involving the Financial Services Authority and financial service institutions—and enhancing repressive protection for customers through more effective mechanisms for complaints, dispute resolution, and loss recovery.*

***Keywords*** *: Legal Protection, Customer Personal Data, Third Parties, Financial Services Sector.*

**Abstrak** : Upaya pemerintah dalam hal perlindungan data pribadi, telah membentuk berbagai instrumen hukum yang mengatur perlindungan data pribadi, penyelenggaraan sistem elektronik, serta tata kelola sektor jasa keuangan yang dituangkan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Selain itu, sebagai Penyelenggara Sistem Elektronik, pelaku usaha di sektor jasa keuangan juga berkewajiban memenuhi ketentuan mengenai keandalan, keamanan, dan perlindungan sistem elektronik sebagaimana diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Namun meskipun demikian, keberadaan berbagai regulasi tersebut perlu dikaji lebih lanjut untuk mengetahui apakah telah memberikan perlindungan hukum yang memadai dalam melindungi data pribadi nasabah pada Penyelenggara Sistem Elektronik di sektor jasa keuangan. Rumusan masalah yang diangkat dalam penelitian ini adalah bagaimana pengaturan hukum tentang perlindungan data pribadi nasabah dalam penyelenggaraan sistem elektronik di sektor jasa keuangan di Indonesia dan bagaimana perlindungan hukum kerahasiaan data pribadi nasabah yang diserahkan kepada kihak ketiga dalam penyelenggaraan sistem elektronik di sektor jasa keuangan. Teori yang digunakan yaitu teori perlindungan hukum dan teori privacy.Metode penelitian yang digunakan yaitu dengan pendekatan hukum yuridis normative yang diperkuat dengan wawancara. Penelitian ini menggunakan pendekatan penelitian Undang-Undang (statute approach), pendekatan kasus (case approach), pendekatan analitis (analytical approach), dan dendekatan konseptual (conceptual approach) yang pada prinsipnya bersumber dari bahan hukum primer terdiri dari undang-undang dan studi kasus, bahan hukum sekunder terdiri buku-buku, hasil-hasil penelitian, artikel serta bahan hukum tersier perpustakaan, artikel dan website. Teknik analisis bahan hukum menggunakan teknik interpretasi gramatikal. Hasil penelitian menunjukan bahwa, pengaturan hukum mengenai pelindungan data pribadi nasabah dalam penyelenggaraan sistem elektronik di sektor jasa keuangan

di Indonesia pada dasarnya telah membentuk kerangka hukum yang memberikan batas terhadap pengumpulan, penyimpanan, penggunaan, dan penyerahan data pribadi kepada pihak lain dan perlindungan hukum terhadap kerahasiaan data pribadi nasabah yang diserahkan kepada pihak ketiga diberikan melalui instrumen preventif dan represif. Saran dari penelitian ini adalah diperlukan penguatan pengaturan dan pengawasan terhadap penyerahan serta pemrosesan data pribadi nasabah oleh pihak ketiga antara Otoritas Jasa Keuangan dengan lembaga jasa keuangan dan perlindungan represif terhadap nasabah perlu diperkuat melalui mekanisme pengaduan, penyelesaian sengketa, dan pemulihan kerugian yang lebih efektif.

**Kata Kunci** : Perlindungan Hukum, Data Pribadi Nasabah, Pihak Ketiga, Sektor Jasa Keuangan .

## PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital pada berbagai sektor kehidupan, termasuk sektor jasa keuangan. Transformasi tersebut ditandai dengan semakin luasnya pemanfaatan penyelenggaraan sistem elektronik dalam penyediaan layanan keuangan, baik oleh perbankan maupun lembaga jasa keuangan lainnya. Berbagai layanan yang sebelumnya dilakukan secara konvensional kini telah beralih ke layanan berbasis digital, seperti pembukaan rekening secara elektronik, layanan *mobile banking*, *internet banking*, pembayaran digital, transaksi investasi, pembiayaan, hingga layanan keuangan berbasis aplikasi. Disisi lain, transformasi digital tersebut menjadikan data pribadi nasabah sebagai salah satu aset yang paling bernilai dalam penyelenggaraan sistem elektronik karena hampir seluruh aktivitas layanan keuangan bergantung pada proses pengumpulan, penggunaan, penyimpanan, dan pengelolaan data pribadi nasabah.[1]

Adapun pengumpulan, penggunaan, penyimpanan, dan bentuk pemrosesan data pribadi tersebut merupakan bagian dari aktivitas pemrosesan data pribadi yang tunduk pada ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (untuk selanjutnya disebut dan/atau ditulis UU PDP), selain itu, sebagai Penyelenggara Sistem Elektronik, pelaku usaha di sektor jasa keuangan juga berkewajiban memenuhi ketentuan mengenai keandalan, keamanan, dan perlindungan sistem elektronik sebagaimana diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Data-data nasabah tidak hanya berfungsi sebagai sarana identifikasi nasabah, tetapi juga menjadi dasar pelaksanaan prinsip kehati-hatian (*prudential principle*), penerapan manajemen risiko, pencegahan tindak pidana pencucian uang, pendanaan terorisme, serta peningkatan kualitas pelayanan kepada konsumen, oleh karena itu, penyelenggara sistem elektronik di sektor jasa keuangan memikul tanggung jawab hukum untuk memastikan bahwa setiap pemrosesan data pribadi dilakukan sesuai dengan prinsip-prinsip perlindungan data pribadi yang diatur dalam

[1] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi; Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

peraturan perundang-undangan.[2] Adapun kewajiban tersebut merupakan implementasi dari hak konstitusional setiap orang untuk memperoleh perlindungan atas diri pribadi, keluarga, kehormatan, martabat, dan rasa aman sebagaimana dijamin dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Dalam konteks perlindungan data pribadi, hak konstitusional tersebut kemudian diimplementasikan lebih lanjut melalui pengaturan mengenai hak subjek data pribadi dan kewajiban Pengendali Data Pribadi dalam UU PDP.

Besarnya ketergantungan sektor jasa keuangan terhadap pemanfaatan sistem elektronik berimplikasi pada meningkatnya risiko terhadap keamanan dan perlindungan data pribadi nasabah. Data pribadi yang tersimpan dalam sistem elektronik memiliki nilai ekonomi yang tinggi sehingga berpotensi menjadi sasaran berbagai bentuk penyalahgunaan, baik melalui akses tanpa hak, pencurian data, manipulasi data, maupun pemanfaatan data untuk melakukan tindak pidana berbasis teknologi informasi. Kondisi tersebut menunjukkan bahwa digitalisasi sektor jasa keuangan tidak hanya menghadirkan peluang bagi peningkatan kualitas pelayanan, tetapi juga melahirkan tantangan baru bagi negara dalam memberikan perlindungan hukum terhadap data pribadi nasabah. Hal ini mengandung makna bahwa keberadaan sistem hukum yang mampu memberikan kepastian hukum terhadap perlindungan data pribadi menjadi salah satu prasyarat penting dalam mewujudkan kepercayaan masyarakat terhadap penyelenggaraan sistem elektronik di sektor jasa keuangan.[3]

Upaya pemerintah dalam hal perlindungan data pribadi, pemerintah telah membentuk berbagai instrumen hukum yang mengatur perlindungan data pribadi, penyelenggaraan sistem elektronik, serta tata kelola sektor jasa keuangan. Namun meskipun demikian, keberadaan berbagai regulasi tersebut perlu dikaji lebih lanjut untuk mengetahui apakah telah memberikan kepastian hukum yang memadai dalam melindungi data pribadi nasabah pada Penyelenggara Sistem Elektronik di sektor jasa keuangan.[4] Keberadaan berbagai pengaturan tersebut menunjukkan bahwa perlindungan data pribadi nasabah pada sektor jasa keuangan tidak hanya berada dalam UU PDP secara umum, tetapi juga menjadi bagian dari Undang-Undang hukum sektor jasa keuangan yang memiliki karakteristik tersendiri. Penyelenggara Sistem Elektronik pada sektor jasa keuangan pada dasarnya tidak hanya berkewajiban memenuhi prinsip-prinsip pemrosesan data pribadi sebagaimana diatur dalam UU PDP, tetapi juga harus mematuhi berbagai ketentuan yang ditetapkan oleh OJK sebagai regulator sektor jasa keuangan. Karakteristik tersebut menunjukkan bahwa perlindungan data pribadi nasabah pada sektor jasa keuangan tidak dapat dipandang semata-mata sebagai bagian dari UU PDP, melainkan juga sebagai bagian dari Undang-Undang hukum sektor jasa keuangan yang berada dalam pengawasan OJK.

Perkembangan penyelenggaraan sistem elektronik pada sektor jasa keuangan yang diikuti dengan meningkatnya penggunaan layanan keuangan digital ternyata juga dibarengi dengan bertambahnya berbagai bentuk penyalahgunaan data pribadi nasabah. Kondisi tersebut tercermin dari meningkatnya pengaduan masyarakat kepada Otoritas Jasa Keuangan (OJK) yang berkaitan dengan penipuan transaksi keuangan, *phishing*, *skimming*, *social engineerizng*, serta perilaku petugas penagihan. Dalam Laporan Kinerja OJK Triwulan II Tahun 2024, permasalahan yang paling banyak dilaporkan oleh masyarakat pada sektor perbankan tidak hanya berkaitan dengan Sistem Layanan Informasi Keuangan (SLIK), tetapi juga mencakup penipuan berupa pembobolan rekening,

[2] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, khususnya ketentuan mengenai prinsip pemrosesan data pribadi, hak subjek data pribadi, serta kewajiban Pengendali Data Pribadi dan Prosesor Data Pribadi.

[3] Jan Michiel Otto, *Shaping the Rule of Law: Considerations from Indonesia* (The Hague: Van Vollenhoven Institute, Leiden University, 2003), hlm. 18–25

[4] Phillipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat di Indonesia* (Surabaya: PT Bina Ilmu, 1987), hlm. 1–5.

*phishing*, *skimming*, dan *social engineering*. Sementara itu, pada sektor Industri Keuangan Non-Bank (IKNB), perilaku petugas penagihan masih menjadi salah satu bentuk pengaduan yang dominan. Data tersebut menunjukkan bahwa persoalan perlindungan data pribadi tidak lagi terbatas pada aspek keamanan teknologi informasi, tetapi telah berkembang menjadi persoalan hukum yang secara langsung memengaruhi keamanan dan kepercayaan masyarakat terhadap penyelenggaraan sistem elektronik di sektor jasa keuangan.[5]

Penulis menelaah fenomena hukum terkait perlindungan data pribadi, Adapun fenomena tersebut penulis uraikan sebagai berikut:

1. Putusan Pengadilan Negeri Sungai Liat Nomor 14/Pid.B/2024/PN Sgl. Dalam perkara tersebut terdapat sejumlah dokumen yang berkaitan dengan data nasabah, termasuk satu bundel data nasabah yang berkaitan dengan penyalahgunaan pencairan, satu bundel data pembiayaan fiktif, serta satu bundel data mengenai penyalahgunaan uang nasabah. Perkara tersebut berkaitan dengan penggunaan data dan dokumen yang berada dalam lingkungan kegiatan perbankan untuk mendukung transaksi pembiayaan dan pencairan yang kemudian dipermasalahkan dalam proses pidana. Data nasabah dan dokumen perbankan menjadi bagian dari barang bukti yang diajukan dalam perkara tersebut.
2. Penggunaan pihak ketiga (*third party*) aplikasi "Mata Elang" (seperti BESTMATEL) bekerja sebagai alat pendukung bagi *debt collector* untuk mencari dan mengidentifikasi kendaraan kredit bermasalah dengan memindai nomor polisi secara *real-time* melalui database dari perusahaan leasing, kemudian membantu mereka melacak, mengintai, dan melakukan penarikan kendaraan di lokasi strategis, di mana data yang diproses mencakup info debitur, kendaraan, hingga ciri-ciri fisik. Terkait dugaan penjualan dan penyalahgunaan data nasabah pembiayaan kendaraan bermotor yang dimanfaatkan oleh pihak tertentu, penanganan terhadap aplikasi yang dimaksud dilakukan sesuai dengan Peraturan Menteri Kominfo Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat.[6]
3. Pemrosesan Data Pribadi Nasabah dalam Penyaluran Kredit Pemilikan Rumah (KPR). Selain perkara penyalahgunaan data dalam kegiatan penagihan dan penyaluran kredit, penelitian ini juga menggunakan kegiatan Kredit Pemilikan Rumah (KPR) sebagai gambaran mengenai pemrosesan data pribadi nasabah yang melibatkan lebih dari satu pihak. Dalam proses pengajuan KPR, calon nasabah harus menyerahkan berbagai informasi dan dokumen untuk kepentingan identifikasi, verifikasi, penilaian kemampuan finansial, dan penilaian kelayakan kredit. Informasi tersebut dapat mencakup identitas diri, informasi pekerjaan, penghasilan, alamat, informasi mengenai status perkawinan, dokumen kepemilikan atau objek yang menjadi jaminan, serta informasi lain yang diperlukan dalam proses pemberian fasilitas kredit. Data yang diperoleh pada tahap pengajuan kemudian digunakan dalam proses pemeriksaan dan penilaian terhadap calon debitur sampai dengan pemberian fasilitas pembiayaan. Setelah hubungan pembiayaan berlangsung, data nasabah juga dapat digunakan untuk kepentingan administrasi, pelayanan, pemantauan pembiayaan, pemenuhan kewajiban hukum, dan kegiatan lain yang berkaitan dengan hubungan pembiayaan.

[5] Otoritas Jasa Keuangan, *Laporan Kinerja OJK Triwulan II Tahun 2024*, Bab VIII mengenai layanan konsumen, yang menunjukkan bahwa penipuan (*phishing*, *skimming*, dan *social engineering*) merupakan salah satu jenis permasalahan yang banyak dilaporkan pada sektor perbankan, sedangkan perilaku petugas penagihan menjadi salah satu pengaduan dominan pada sektor IKNB

[6] KOMDIGI, *Kemkomdigi Tindak Delapan Aplikasi Diduga Menyalahgunakan Data Nasabah Pembiayaan,* https://www.komdigi.go.id/berita/siaran-pers/detail/kemkomdigi-tindak-delapan-aplikasi-diduga-menyalahgunakan-data-nasabah-pembiayaan [diakses pada 25/07/2026 pukul 14:21 WIB]

Berdasarkan Laporan Kinerja OJK Triwulan II Tahun 2024 menunjukkan bahwa salah satu jenis sengketa yang banyak diterima oleh Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK) berkaitan dengan perilaku petugas penagihan, sementara fraud eksternal seperti penipuan, pembobolan rekening, *skimming*, dan *cyber crime* juga termasuk dalam kelompok sengketa yang dominan. Pada periode yang sama, Satgas PASTI menerima ribuan pengaduan masyarakat terkait aktivitas keuangan ilegal, terutama pinjaman online ilegal, serta melakukan penghentian terhadap ribuan entitas ilegal, pemblokiran rekening bank, dan ratusan nomor kontak pihak penagih yang terkait dengan aktivitas tersebut. Fakta tersebut menunjukkan bahwa penyalahgunaan data pribadi dan penyalahgunaan layanan keuangan digital bukan lagi merupakan peristiwa yang bersifat insidental, melainkan telah berkembang menjadi persoalan yang memerlukan perhatian serius dari regulator sektor jasa keuangan.[7]

## METODE PENELITIAN

Metode penelitian yang digunakan yaitu dengan pendekatan hukum yuridis normative yang diperkuat dengan wawancara. Penelitian ini menggunakan pendekatan penelitian Undang-Undang (*statute approach*), pendekatan kasus (*case approach*), pendekatan analitis (*analytical approach*), dan dendekatan konseptual (*conceptual approach*) yang pada prinsipnya bersumber dari bahan hukum primer terdiri dari undang-undang dan studi kasus, bahan hukum sekunder terdiri buku-buku, hasil-hasil penelitian, artikel serta bahan hukum tersier perpustakaan, artikel dan website. Teknik analisis bahan hukum menggunakan teknik interpretasi gramatikal.

## HASIL DAN PEMBAHASAN

### Pengaturan Hukum Tentang Perlindungan Data Pribadi Nasabah Dalam Penyelenggaraan Sistem Elektronik Di Sektor Jasa Keuangan Di Indonesia.

Aturan hukum perlindungan data pribadi nasabah dalam penyelenggaraan sistem elektronik di sektor jasa keuangan Indonesia yang semakin kompleks seiring dengan digitalisasi layanan keuangan. Penggunaan sistem elektronik dalam pembukaan rekening, verifikasi identitas, pembiayaan, transaksi, pelayanan konsumen, hingga penagihan menyebabkan PUJK melakukan pengumpulan dan pemrosesan data dalam jumlah besar. Data tersebut tidak hanya meliputi identitas dasar, tetapi juga informasi rekening, riwayat transaksi, kredit atau pembiayaan, serta informasi kondisi ekonomi nasabah. Dalam kerangka Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), data keuangan pribadi dikategorikan sebagai data pribadi yang bersifat spesifik sehingga membutuhkan tingkat perlindungan yang lebih tinggi.

Dalam perspektif teori privasi Alan F. Westin, privasi dipahami sebagai hak individu untuk menentukan kapan, bagaimana, dan sejauh mana informasi mengenai dirinya dikomunikasikan kepada pihak lain. Teori ini sangat relevan dalam hubungan antara nasabah dan PUJK karena pemberian data oleh nasabah pada dasarnya dilakukan untuk tujuan tertentu, bukan sebagai penyerahan kewenangan tanpa batas kepada PUJK. Dengan demikian, ketika nasabah memberikan data untuk memperoleh layanan pembiayaan atau perbankan, persetujuan tersebut tidak otomatis dapat dimaknai sebagai izin untuk menggunakan atau mengungkapkan data kepada pihak lain untuk segala macam kepentingan. Perlindungan privasi menurut Westin bertumpu pada tetap terjaganya kontrol individu terhadap informasi mengenai dirinya.

[7] Otoritas Jasa Keuangan, *Laporan Kinerja OJK Triwulan II Tahun 2024*, Bab VIII. Laporan tersebut menunjukkan bahwa sengketa mengenai perilaku petugas penagihan serta *fraud* eksternal (penipuan, pembobolan rekening, *skimming*, dan *cyber crime*) termasuk dalam jenis sengketa yang dominan. Selain itu, Satgas PASTI menerima 3.306 pengaduan pada Triwulan II 2024, menghentikan 1.191 entitas pinjaman online ilegal, memblokir 185 rekening bank dan 801 nomor kontak pihak penagih yang terkait dengan aktivitas pinjaman online ilegal.

Persoalan kontrol tersebut menjadi semakin penting ketika penyelenggaraan jasa keuangan melibatkan pihak ketiga, seperti penyedia teknologi informasi, pengelola data, penyedia infrastruktur, maupun perusahaan penagihan. Data nasabah dapat berpindah dari penguasaan langsung PUJK ke dalam suatu rantai pemrosesan yang lebih luas. Karena itu, persoalan hukumnya bukan hanya apakah PUJK memperoleh data secara sah, tetapi apakah setelah diperoleh data tersebut tetap digunakan sesuai tujuan, dasar, dan batas yang dapat dipahami oleh nasabah. PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik memasukkan transfer, penyebarluasan, dan pengungkapan data sebagai bagian dari pemrosesan data pribadi sehingga perpindahan data kepada pihak lain tetap berada dalam ruang lingkup kewajiban pelindungan data.

UU PDP kemudian memberikan dasar normatif melalui Pasal 20, yang mewajibkan Pengendali Data Pribadi memiliki dasar pemrosesan. Dasar tersebut dapat berupa persetujuan yang sah, pelaksanaan perjanjian, pemenuhan kewajiban hukum, perlindungan kepentingan vital, kepentingan umum, maupun kepentingan yang sah sesuai dengan persyaratan undang-undang. Ketentuan tersebut menegaskan bahwa penguasaan faktual atas data tidak sama dengan kewenangan hukum untuk menggunakan data secara bebas. Data nasabah yang diperoleh untuk pembukaan rekening, pembiayaan, transaksi, atau pelayanan tertentu tidak dengan sendirinya dapat digunakan untuk tujuan lain apabila tidak terdapat dasar pemrosesan yang sah.

UU PDP juga membangun perlindungan melalui kewajiban keamanan dan kerahasiaan data. Pasal 35 mewajibkan Pengendali Data Pribadi melindungi dan memastikan keamanan data melalui langkah teknis dan operasional yang sesuai dengan sifat serta risiko data. Pasal 36 mewajibkan pengendali menjaga kerahasiaan data pribadi, sedangkan Pasal 37 mewajibkan pengendali melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan di bawah kendalinya. Dengan demikian, keterlibatan pihak ketiga tidak menghapus tanggung jawab PUJK untuk memastikan data nasabah tetap diproses secara sah, aman, dan sesuai tujuan.

Pengaturan tersebut diperkuat oleh POJK Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Peraturan ini mewajibkan PUJK menjaga kerahasiaan dan keamanan data dan/atau informasi konsumen serta mengatur pertukaran data dengan pihak lain. Transfer data mencakup perpindahan, pengiriman, dan/atau penggandaan data pribadi dari PUJK kepada pihak lain. Dengan demikian, hukum sektor jasa keuangan mengakui bahwa pertukaran data dapat diperlukan dalam kegiatan usaha, tetapi pertukaran tersebut tetap harus berada dalam batas hukum pelindungan data pribadi dan tidak menghilangkan hak konsumen atas kerahasiaan serta kontrol terhadap datanya.

Selain teori Westin, analisis menggunakan teori perlindungan hukum Philipus M. Hadjon, yang membedakan perlindungan hukum menjadi perlindungan preventif dan represif. Perlindungan preventif diberikan melalui pembentukan norma yang membatasi tindakan sebelum terjadi sengketa atau pelanggaran, sedangkan perlindungan represif diberikan setelah terjadi pelanggaran. Dalam konteks perlindungan data nasabah, bentuk preventif terlihat dalam kewajiban memiliki dasar pemrosesan, memberikan informasi kepada subjek data, menjaga kerahasiaan, menerapkan keamanan, membatasi pertukaran data, serta melakukan pengawasan terhadap pihak ketiga. Teori Hadjon digunakan untuk menjelaskan bagaimana hukum memberikan perlindungan, sedangkan teori Westin digunakan untuk menjelaskan apa yang harus dilindungi, yaitu kontrol individu atas informasi pribadinya.

Kedua teori tersebut juga memberikan dasar untuk menilai keabsahan persetujuan nasabah. Dalam perspektif Westin, persetujuan baru memiliki makna substantif apabila nasabah mengetahui informasi apa yang dikomunikasikan, kepada siapa informasi diberikan, untuk tujuan apa informasi

digunakan, dan sejauh mana komunikasi dilakukan. Persetujuan yang terlalu umum, khususnya dalam perjanjian baku dan sistem elektronik, berpotensi menjadikan privasi sekadar formalitas administratif. Karena itu, Pasal 5 UU PDP yang memberikan hak kepada subjek data untuk memperoleh informasi mengenai identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data, serta akuntabilitas pihak yang meminta data mempunyai arti penting dalam menjaga kontrol nasabah.

Konsep purpose limitation juga menjadi bagian penting dalam analisis. Meskipun UU PDP tidak secara khusus menggunakan istilah tersebut sebagai prinsip tersendiri, substansinya tercermin dalam pengaturan mengenai dasar dan tujuan pemrosesan, relevansi data, serta kewajiban pengendali. Semakin luas penggunaan data tanpa tujuan yang jelas, semakin kecil kemampuan nasabah untuk mengetahui dan mengendalikan informasi mengenai dirinya. Sebaliknya, semakin spesifik tujuan dan batas pemrosesan, semakin kuat kontrol subjek data. Dalam perspektif Hadjon, kewajiban PUJK menetapkan batas pemrosesan dan mengawasi pihak ketiga merupakan bentuk perlindungan preventif untuk mencegah penggunaan kewenangan secara sewenang-wenang.

UU PDP juga membedakan kedudukan Pengendali Data Pribadi dan Prosesor Data Pribadi. Pengendali menentukan tujuan dan melakukan kendali terhadap pemrosesan, sedangkan Prosesor melakukan pemrosesan berdasarkan perintah Pengendali. Dalam hubungan PUJK dengan pihak ketiga, penentuan kedudukan tersebut tidak cukup berdasarkan nama atau bentuk kontrak, tetapi harus dilihat dari siapa yang menentukan tujuan dan cara pemrosesan serta untuk kepentingan siapa pemrosesan dilakukan. Pembedaan ini penting karena menentukan ruang kewenangan dan pertanggungjawaban masing-masing pihak dalam rantai pemrosesan data.

Dalam konteks tersebut, POJK Nomor 22 Tahun 2023 memperkuat kewajiban PUJK ketika menggunakan pihak ketiga. PUJK harus memastikan bahwa pihak yang bekerja sama dengannya tetap menjaga kerahasiaan dan keamanan data konsumen. Pertukaran data dengan pihak lain juga harus memperhatikan UU PDP dan ketentuan OJK serta, dalam kondisi tertentu, mensyaratkan persetujuan konsumen secara tertulis dan/atau kewajiban berdasarkan peraturan perundang-undangan. Hal tersebut menunjukkan bahwa hubungan kontraktual dengan pihak ketiga tidak cukup untuk membebaskan PUJK dari tanggung jawab perlindungan data.

Perbandingan dengan hukum internasional menunjukkan bahwa Indonesia memiliki konstruksi yang sejalan dengan perkembangan global. General Data Protection Regulation (GDPR) Uni Eropa secara tegas membedakan controller dan processor serta mengatur kewajiban controller dalam memilih processor, menjamin kemampuan perlindungan data, membatasi pemrosesan berdasarkan instruksi, dan mengendalikan sub-processor. GDPR juga menekankan prinsip akuntabilitas sehingga organisasi tidak hanya diwajibkan mematuhi aturan, tetapi harus mampu menunjukkan bahwa pemrosesannya telah memenuhi prinsip perlindungan data.

Pendekatan Amerika Serikat melalui California Consumer Privacy Act (CCPA) lebih terfragmentasi dibandingkan GDPR, tetapi tetap memberikan konsumen hak untuk mengontrol bagaimana data pribadi dikumpulkan, digunakan, dan dibagikan. Sementara itu, negara-negara ASEAN seperti Malaysia dan Singapura juga membangun mekanisme perlindungan yang relevan. Malaysia melalui *Personal Data Protection Act* dan perubahan tahun 2024 memperkuat kewajiban penunjukan Data Protection Officer. Singapura melalui Personal Data Protection Act 2012 (PDPA) membedakan organisasi dengan data intermediary dan tetap menempatkan organisasi sebagai pihak yang bertanggung jawab terhadap data yang diproses atas namanya.

Perbandingan Indonesia, Uni Eropa, dan Singapura memperlihatkan kesamaan bahwa penggunaan pihak ketiga tidak dilarang, tetapi harus disertai pembatasan tujuan, kejelasan kedudukan para pihak, pengawasan, dan pertanggungjawaban. Perbedaannya terletak pada tingkat

kerincian mekanisme pengendalian. GDPR memberikan pengaturan yang lebih detail mengenai seleksi processor, instruksi pemrosesan, dan sub-processor, sementara Singapura menekankan tanggung jawab organisasi atas pemrosesan yang dilakukan data intermediary. Indonesia telah mempunyai fondasi melalui konsep Pengendali dan Prosesor dalam UU PDP, tetapi masih perlu penguatan penerapan terhadap rantai pemrosesan yang kompleks di sektor jasa keuangan.

Kasus yang relevan dengan persoalan tersebut adalah dugaan penyalahgunaan data nasabah pembiayaan kendaraan bermotor melalui aplikasi digital pada Desember 2025. Kementerian Komunikasi dan Digital menindaklanjuti dugaan penyebaran data objek fidusia secara tidak sah dan mengajukan delapan aplikasi untuk dihapus dari platform digital, dengan beberapa aplikasi telah tidak aktif ketika pernyataan tersebut disampaikan. Data yang disebut diproses antara lain informasi debitur, kendaraan, dan ciri-ciri fisik kendaraan. Peristiwa ini tidak digunakan untuk menyimpulkan bahwa seluruh pihak yang terlibat telah terbukti melanggar hukum, tetapi menunjukkan risiko hilangnya kontrol nasabah ketika data masuk ke rantai pemrosesan yang melibatkan pihak lain.

Fenomena Bestmatel dalam kegiatan penagihan juga memperlihatkan persoalan serupa. Aplikasi tersebut disebut digunakan untuk membantu debt collector mencari dan mengidentifikasi kendaraan bermasalah melalui pemindaian nomor polisi secara real-time, dengan informasi yang diproses mencakup data debitur, kendaraan, dan ciri-ciri fisik tertentu. Persoalan hukumnya bukan semata-mata mengenai kegiatan penagihan, tetapi mengenai asal-usul data, kewenangan pihak yang memperoleh akses, tujuan penggunaannya, dan mekanisme pengawasan. Dari perspektif Westin, penggunaan informasi untuk mengidentifikasi dan melacak seseorang harus tetap diuji berdasarkan tujuan awal ketika data tersebut diberikan oleh nasabah.

Hasil wawancara dengan Ibu Ria selaku pimpinan cabang perusahaan pembiayaan memberikan gambaran praktik hubungan PUJK dengan pihak ketiga dalam kegiatan penagihan. Berdasarkan wawancara tersebut, perusahaan pembiayaan bekerja sama dengan pihak ketiga yang berbadan hukum, tetapi perusahaan tidak mengetahui secara rinci cara pihak ketiga melakukan penagihan dan setelah memberikan data nasabah tidak melakukan pengawasan terhadap pihak tersebut. Kerja sama dengan pihak ketiga sendiri tidak otomatis bertentangan dengan hukum sepanjang dilakukan sesuai ketentuan. Persoalan utamanya terletak pada lemahnya pengawasan terhadap data yang telah diberikan atau dapat diakses pihak ketiga sehingga membuka risiko penggunaan atau pengungkapan data di luar tujuan penagihan.

Kasus lain berkaitan dengan pemrosesan data nasabah dalam Kredit Pemilikan Rumah (KPR). Dalam penyelenggaraan pembiayaan KPR, bank dapat melibatkan pihak ketiga untuk fungsi administratif, pengelolaan dokumen, penagihan, maupun fungsi pendukung lainnya. Perpindahan data dalam kondisi tersebut tidak otomatis merupakan pelanggaran UU PDP karena dapat menjadi bagian dari pemrosesan yang sah. Namun, pihak ketiga hanya boleh memproses data berdasarkan tujuan dan kewenangan yang telah ditentukan. Penggunaan data untuk kepentingan lain, seperti pemasaran, pembentukan profil, atau pemberian kepada pihak lain tanpa dasar pemrosesan yang sah, dapat menimbulkan function creep, yaitu penggunaan data untuk tujuan yang berbeda dari tujuan awal.

Kasus berikutnya adalah Putusan Pengadilan Negeri Sungai Liat Nomor 14/Pid.B/2024/PN Sgl mengenai kredit fiktif yang dilakukan oleh pegawai bank. Perkara tersebut menunjukkan bahwa ancaman penyalahgunaan data nasabah tidak hanya berasal dari pihak ketiga, tetapi juga dapat berasal dari internal lembaga keuangan sendiri. Dalam perkara tersebut terdapat barang bukti berupa data nasabah yang berkaitan dengan penyalahgunaan pencairan, pembiayaan fiktif, dan penyalahgunaan uang nasabah. Dari perspektif UU PDP, bank sebagai Pengendali Data Pribadi tetap

berkewajiban memastikan siapa yang memperoleh akses, tujuan akses, tindakan yang dapat dilakukan terhadap data, dan bagaimana penggunaan akses tersebut diawasi.

Pada akhirnya, perlindungan hukum terhadap data pribadi nasabah harus dipahami sebagai perlindungan sepanjang siklus pemrosesan data, mulai dari pengumpulan, penyimpanan, akses, penggunaan, transfer, pengungkapan, hingga penghapusan atau pemusnahan. Pasal 47 UU PDP menempatkan tanggung jawab pemrosesan pada Pengendali Data Pribadi, sedangkan Pasal 12 UU PDP memberikan hak kepada subjek data untuk menggugat dan menerima ganti rugi apabila terjadi pelanggaran pemrosesan data pribadi. Selain itu, UU PDP menyediakan sanksi administratif dan pidana terhadap bentuk-bentuk pelanggaran tertentu. Dengan demikian, teori Hadjon menunjukkan bahwa perlindungan data harus dibangun melalui mekanisme preventif sekaligus represif, sedangkan teori Westin menegaskan bahwa tujuan utama perlindungan tersebut adalah mempertahankan kontrol individu atas informasi pribadinya. Konstruksi UU PDP, PP Nomor 71 Tahun 2019, POJK Nomor 22 Tahun 2023, serta regulasi pendukung OJK pada akhirnya menunjukkan bahwa perpindahan data nasabah kepada pihak ketiga tidak dilarang secara mutlak, tetapi harus mempunyai dasar pemrosesan yang sah, tujuan yang jelas, akses yang terbatas, keamanan dan kerahasiaan yang terjamin, serta pengawasan dan pertanggungjawaban yang memadai.

**Perlindungan Hukum Kerahasiaan Data Pribadi Nasabah Dalam Penyelenggaraan Sitem Elektronik Di Sektor Jasa Keuangan Di Indonesia**

Perlindungan hukum terhadap kerahasiaan data pribadi nasabah yang diserahkan kepada pihak ketiga dalam penyelenggaraan sistem elektronik di sektor jasa keuangan pada dasarnya berangkat dari konsep privasi sebagai bagian dari hak yang harus dilindungi. Alan F. Westin memandang privasi sebagai hak individu untuk menentukan apakah informasi mengenai dirinya dikomunikasikan kepada pihak lain atau tidak. Pemikiran tersebut menempatkan data pribadi sebagai bagian dari *information privacy*, karena individu memiliki kepentingan untuk mengetahui, mengendalikan, dan menentukan penggunaan informasi mengenai dirinya. Konsep ini menjadi dasar penting dalam menilai sejauh mana data nasabah dapat diberikan, diproses, dan digunakan oleh pihak ketiga.

Konsep privasi juga berkembang dari pemikiran Warren dan Brandeis mengenai *the right to privacy*, yaitu hak individu untuk tidak diganggu dalam kehidupan pribadinya. Perkembangan teknologi memperluas makna privasi karena informasi pribadi dapat dikumpulkan, disimpan, dipindahkan, dan diproses oleh berbagai pihak dengan cepat. Dalam konteks jasa keuangan, hak atas privasi tidak hanya berarti bahwa data harus dirahasiakan, tetapi juga mencakup hak nasabah untuk mengetahui siapa yang mengakses datanya, untuk tujuan apa data digunakan, bagaimana data diproses dan disimpan, serta hak untuk memberikan atau menolak persetujuan sesuai dengan ketentuan hukum.

Digitalisasi sektor jasa keuangan menyebabkan hubungan antara Pelaku Usaha Jasa Keuangan (PUJK) dengan nasabah semakin bergantung pada sistem elektronik. Data pribadi nasabah dapat dikumpulkan dan diproses sejak proses pengajuan layanan hingga pelaksanaan transaksi dan pelayanan setelah transaksi berlangsung. Kondisi tersebut memberikan kemudahan bagi penyelenggara jasa keuangan, tetapi sekaligus memperbesar kemungkinan data diakses atau diproses oleh pihak lain yang tidak berhubungan langsung dengan nasabah. Karena itu, data pribadi nasabah memiliki kedudukan hukum yang harus mendapatkan perlindungan khusus, terutama karena dapat memuat identitas, alamat, informasi pembiayaan, dan kondisi ekonomi seseorang.

Secara normatif, perlindungan tersebut diperkuat oleh Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. POJK Nomor

22 Tahun 2023 menegaskan bahwa data dan informasi konsumen wajib dijaga kerahasiaan dan keamanannya oleh PUJK. Bahkan ketika PUJK bekerja sama dengan pihak lain untuk mengelola data konsumen, PUJK tetap berkewajiban memastikan pihak tersebut menjaga kerahasiaan dan keamanan data. UU PDP juga memberikan kewajiban kepada Pengendali Data Pribadi untuk menjaga kerahasiaan, keamanan, serta melakukan pengawasan terhadap pihak yang terlibat dalam pemrosesan.

Salah satu kasus yang memperlihatkan persoalan tersebut adalah penggunaan aplikasi Bestmatel dalam kegiatan penagihan oleh pihak ketiga. Sistem tersebut memungkinkan informasi mengenai nasabah dan objek pembiayaan tersedia dan diakses melalui sistem elektronik. Persoalan hukumnya bukan hanya berkaitan dengan kegiatan penagihan, tetapi juga mengenai bagaimana data diperoleh, siapa yang memiliki kewenangan mengakses, untuk tujuan apa data digunakan, dan bagaimana PUJK melakukan pengawasan terhadap pihak yang memproses data tersebut. Kasus ini menunjukkan bahwa penyerahan data kepada pihak ketiga dapat menimbulkan persoalan hukum apabila kontrol terhadap data tidak tetap dipertahankan.

Pada Desember 2025, Kementerian Komunikasi dan Digital juga menindaklanjuti dugaan penyalahgunaan data nasabah pembiayaan kendaraan bermotor yang beredar melalui aplikasi digital. Pemerintah menyatakan terdapat indikasi penyebaran data objek fidusia secara tidak sah dan mengajukan delapan aplikasi yang berkaitan dengan praktik Mata Elang untuk dihapus dari platform digital. Aplikasi seperti BESTMATEL disebut digunakan untuk membantu *debt collector* mencari dan mengidentifikasi kendaraan bermasalah melalui pemindaian nomor polisi secara *real-time*. Informasi yang diproses antara lain data debitur, kendaraan, dan ciri-ciri fisik tertentu.

Fenomena tersebut memperlihatkan bahwa data yang pada awalnya dikumpulkan untuk kepentingan hubungan pembiayaan dapat berubah fungsi menjadi instrumen untuk mengidentifikasi dan melacak debitur serta objek pembiayaan. Dari perspektif teori privasi Alan F. Westin, keadaan tersebut harus diuji berdasarkan tujuan awal pemberian data. Nasabah yang memberikan informasi kepada perusahaan pembiayaan untuk memperoleh layanan tidak serta-merta memberikan kewenangan tanpa batas kepada pihak lain untuk menggunakan informasi tersebut. Semakin luas akses dan penggunaan data oleh pihak ketiga, semakin besar pula potensi berkurangnya kontrol nasabah terhadap informasi pribadinya.

Dalam perspektif teori perlindungan hukum Philipus M. Hadjon, perlindungan terhadap data nasabah terdiri atas perlindungan hukum preventif dan represif. Perlindungan preventif bertujuan mencegah terjadinya pelanggaran melalui kewajiban hukum sebelum kerugian terjadi. Dalam konteks UU PDP, bentuk perlindungan preventif antara lain terlihat dalam kewajiban melakukan penilaian dampak pelindungan data pribadi sebagaimana Pasal 34, terutama terhadap pemrosesan berisiko tinggi seperti pemrosesan dalam skala besar, pemantauan sistematis, pencocokan atau penggabungan data, penggunaan teknologi baru, dan pemrosesan yang membatasi hak subjek data pribadi.

Kewajiban preventif tersebut menjadi penting ketika teknologi memungkinkan penggabungan berbagai informasi untuk mengidentifikasi seseorang. Risiko tidak dapat dinilai hanya berdasarkan masing-masing data secara terpisah, tetapi juga harus mempertimbangkan kemampuan sistem menghasilkan informasi baru melalui penggabungan data. Karena itu, Pengendali Data Pribadi harus mempertimbangkan kemungkinan akses yang terlalu luas, penggunaan data di luar tujuan, dan kesulitan mengendalikan data setelah berada dalam sistem pihak ketiga. Kewajiban tersebut diperkuat oleh Pasal 35 UU PDP mengenai keamanan data dan Pasal 37 mengenai kewajiban Pengendali melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan.

Pengawasan terhadap pihak ketiga juga ditegaskan dalam POJK Nomor 22 Tahun 2023. Pasal 19 ayat (4) mengharuskan PUJK yang bekerja sama dengan pihak lain untuk mengelola data dan/atau informasi konsumen memastikan pihak tersebut menjaga kerahasiaan dan keamanan data. Kewajiban tersebut kemudian diperkuat melalui SEOJK Nomor 18/SEOJK.08/2024 yang menjadikan pengelolaan pihak ketiga sebagai bagian dari penilaian terhadap kepatuhan PUJK, termasuk keberadaan kebijakan atau prosedur tertulis yang memastikan pihak ketiga menerapkan prinsip dasar pemrosesan data pribadi. Hal tersebut menunjukkan adanya kewajiban *due diligence* terhadap pihak ketiga.

Hasil wawancara dengan Ibu Ria selaku pimpinan cabang sebuah perusahaan pembiayaan memberikan gambaran mengenai praktik kerja sama dengan pihak ketiga dalam kegiatan penagihan. Berdasarkan wawancara tersebut, perusahaan pembiayaan bekerja sama dengan pihak ketiga yang berbadan hukum, tetapi perusahaan tidak mengetahui secara rinci cara pihak ketiga melakukan penagihan dan tidak melakukan pengawasan setelah data nasabah diberikan. Kerja sama tersebut pada dasarnya tidak bertentangan dengan hukum selama dilakukan sesuai ketentuan yang berlaku. Permasalahan hukumnya terletak pada lemahnya pengawasan sehingga data berpotensi digunakan, diakses, atau diungkapkan di luar tujuan penagihan.

Keadaan tersebut menunjukkan relevansi teori perlindungan hukum Philipus M. Hadjon. Perlindungan preventif seharusnya diwujudkan melalui pembatasan jenis data yang diberikan kepada pihak ketiga, penentuan tujuan penggunaan, mekanisme pengamanan, serta pengawasan selama kegiatan penagihan berlangsung. Apabila pelanggaran telah terjadi, perlindungan represif diperlukan untuk memberikan pertanggungjawaban dan pemulihan terhadap nasabah. Sementara itu, menurut teori privasi Alan F. Westin, pemberian data untuk tujuan penagihan tidak dapat dimaknai sebagai pelepasan kontrol nasabah atas seluruh informasi pribadinya.

Persoalan perpindahan data juga dapat dilihat dalam kegiatan pemrosesan data nasabah Kredit Pemilikan Rumah (KPR). Dalam penyelenggaraan KPR, bank dapat melibatkan pihak ketiga dalam kegiatan administratif, pengelolaan dokumen, penagihan, maupun fungsi pendukung lainnya. Dalam konteks perbankan digital, kerja sama dengan pihak ketiga yang melakukan pemrosesan data pribadi harus didukung perjanjian yang jelas mengenai ruang lingkup dan durasi pemrosesan, tujuan pemrosesan, jenis data yang diproses, kategori nasabah, serta hak dan kewajiban Pengendali Data Pribadi.

Perpindahan data dalam kegiatan KPR tidak secara otomatis merupakan pelanggaran UU PDP. Persoalan hukumnya terletak pada apakah perpindahan tersebut mempunyai dasar pemrosesan yang sah dan tetap berada dalam tujuan pemrosesan yang dibenarkan. Data calon debitur dapat meliputi identitas, alamat, pekerjaan, penghasilan, kondisi keuangan, serta dokumen lain yang diperlukan untuk analisis pembiayaan. Ketika data tersebut diproses pihak ketiga, pihak tersebut tidak memperoleh kebebasan untuk menentukan sendiri penggunaan data hanya karena data telah diserahkan oleh bank. Transfer, pengungkapan, dan penggunaan tetap merupakan bagian dari pemrosesan yang tunduk pada ketentuan pelindungan data pribadi.

Pembatasan akses menjadi penting untuk mencegah terjadinya *function creep*, yaitu keadaan ketika data yang dikumpulkan untuk satu tujuan kemudian digunakan untuk tujuan lain yang tidak lagi memiliki hubungan memadai dengan tujuan awal. Data nasabah yang diberikan untuk kepentingan administrasi KPR, misalnya, tidak secara otomatis dapat digunakan untuk pemasaran produk lain, diberikan kepada pihak lain, atau digunakan untuk membentuk profil nasabah apabila tidak terdapat dasar pemrosesan yang sah. Karena itu, tujuan pemrosesan harus menjadi instrumen pembatas terhadap penggunaan data oleh bank maupun pihak ketiga.

Dalam hubungan bank dengan pihak ketiga, bank sebagai Pengendali Data Pribadi tetap bertanggung jawab memastikan pihak yang memproses data bertindak sesuai instruksi dan tujuan yang telah ditentukan. Hal ini sejalan dengan POJK Nomor 22 Tahun 2023 yang mewajibkan PUJK menjaga kerahasiaan dan keamanan data konsumen serta memastikan pihak lain yang bekerja sama dengannya melakukan kewajiban yang sama. Dengan demikian, keterlibatan pihak ketiga tidak menghilangkan kewajiban PUJK untuk melindungi data nasabah. Dalam perspektif Hadjon, kewajiban tersebut merupakan bentuk perlindungan hukum preventif karena negara menetapkan prosedur, pembatasan akses, perjanjian, dan pengawasan sebelum kerugian terjadi.

Kasus lain yang penting adalah Putusan Pengadilan Negeri Sungai Liat Nomor 14/Pid.B/2024/PN Sgl mengenai kredit fiktif yang dilakukan oleh pegawai bank. Dalam perkara tersebut, terdakwa Sumiani dinyatakan terbukti melakukan tindak pidana sebagai pegawai bank syariah dengan membuat pencatatan palsu dalam pembukuan dan laporan transaksi bank syariah. Barang bukti perkara antara lain mencantumkan data nasabah terkait penyalahgunaan pencairan, data pembiayaan fiktif, dan data penyalahgunaan uang nasabah. Kasus tersebut memperlihatkan bahwa ancaman terhadap kerahasiaan dan keamanan data tidak hanya berasal dari pihak ketiga, tetapi juga dapat berasal dari internal lembaga keuangan.

Dari perspektif UU PDP, bank sebagai Pengendali Data Pribadi mempunyai tanggung jawab terhadap pemrosesan data sebagaimana ditegaskan dalam Pasal 47. Keamanan data tidak cukup dinilai dari kemampuan sistem menyimpan data secara aman, tetapi juga harus mencakup siapa yang mempunyai akses, tujuan pemberian akses, tindakan yang dapat dilakukan terhadap data, serta mekanisme pengawasan terhadap penggunaan akses tersebut. Dengan demikian, perlindungan data pribadi merupakan bagian dari tata kelola internal lembaga jasa keuangan. Keabsahan bank dalam memperoleh dan menyimpan data tidak memberikan legitimasi kepada pegawai atau pihak lain untuk menggunakan data secara bebas.

Perlindungan hukum kemudian harus mencakup seluruh siklus pemrosesan data, mulai dari data diperoleh, disimpan, diakses, digunakan, diserahkan kepada pihak lain, sampai dengan dihapus atau dimusnahkan. Kegagalan pada salah satu tahapan tersebut dapat membuka peluang terjadinya penyalahgunaan dan menimbulkan konsekuensi hukum. Dalam konteks teori Hadjon, perlindungan preventif harus mencegah pelanggaran sejak awal, sedangkan perlindungan represif diperlukan ketika pencegahan tidak berhasil. Perlindungan represif tidak hanya berupa sanksi, tetapi juga harus memberikan mekanisme pemulihan bagi nasabah yang haknya telah dilanggar.

Instrumen perlindungan represif salah satunya terdapat dalam Pasal 12 UU PDP yang memberikan hak kepada subjek data pribadi untuk menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi mengenai dirinya. Selain itu, UU PDP menyediakan sanksi administratif berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan, penghapusan atau pemusnahan data, dan denda administratif. UU PDP juga mengatur ketentuan pidana terhadap perbuatan tertentu, antara lain memperoleh, mengumpulkan, mengungkapkan, atau menggunakan data pribadi yang bukan miliknya secara melawan hukum. Ketentuan tersebut menunjukkan bahwa perlindungan represif memiliki fungsi memberikan konsekuensi kepada pelanggar sekaligus menyediakan jalan pemulihan bagi pemilik data.

Pada akhirnya, berdasarkan teori perlindungan hukum Philipus M. Hadjon dan teori privasi Alan F. Westin, perlindungan kerahasiaan data pribadi nasabah dalam penyelenggaraan sistem elektronik sektor jasa keuangan harus dibangun melalui keseimbangan antara kebutuhan PUJK memproses data dan hak nasabah untuk tetap memiliki kontrol terhadap informasi pribadinya. Penyerahan data kepada pihak ketiga tidak dilarang sepanjang mempunyai dasar hukum, tujuan yang jelas, akses yang terbatas, keamanan dan kerahasiaan yang terjamin, serta pengawasan yang

memadai. Ketika data digunakan di luar tujuan, diakses tanpa kewenangan, atau diungkapkan secara tidak sah, mekanisme represif harus dapat memberikan pemulihan, ganti rugi, dan sanksi. Dengan demikian, efektivitas perlindungan hukum tidak hanya ditentukan oleh keberadaan larangan, tetapi juga oleh kemampuan hukum menyediakan pengaduan, penyelesaian sengketa, tuntutan ganti rugi, serta pertanggungjawaban terhadap pihak yang menyalahgunakan data.

**KESIMPULAN**

1. Pengaturan hukum mengenai pelindungan data pribadi nasabah dalam penyelenggaraan sistem elektronik di sektor jasa keuangan di Indonesia pada dasarnya telah membentuk kerangka hukum yang memberikan batas terhadap pengumpulan, penyimpanan, penggunaan, dan penyerahan data pribadi kepada pihak lain. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi menempatkan pemrosesan data harus dilakukan berdasarkan dasar pemrosesan yang sah, tujuan yang jelas, serta prinsip pelindungan data pribadi. Dalam konteks sektor jasa keuangan, pengaturan tersebut berhubungan dengan kewajiban lembaga jasa keuangan dalam menjaga kerahasiaan, keamanan, dan penggunaan data nasabah. Penyerahan data kepada pihak ketiga dengan demikian bukan merupakan tindakan yang secara mutlak dilarang, tetapi harus dibatasi oleh tujuan dan dasar pemrosesan yang sah serta disertai pengawasan terhadap pihak yang menerima atau memproses data. Permasalahan muncul ketika data yang telah diserahkan atau diberikan akses kepada pihak lain digunakan di luar tujuan yang sah, sebagaimana dapat dilihat dari berbagai fenomena penyalahgunaan data dalam praktik sektor jasa keuangan. Kondisi tersebut menunjukkan masih terdapat kesenjangan antara konstruksi normatif yang menghendaki pengendalian terhadap seluruh proses pemrosesan data dengan praktik yang memungkinkan terjadinya penyalahgunaan data setelah data berada dalam penguasaan pihak lain.
2. Perlindungan hukum terhadap kerahasiaan data pribadi nasabah yang diserahkan kepada pihak ketiga diberikan melalui instrumen preventif dan represif. Perlindungan preventif diwujudkan melalui pembatasan tujuan dan dasar pemrosesan, kewajiban menjaga kerahasiaan dan keamanan data, pengawasan terhadap pihak yang melakukan pemrosesan, serta pembatasan penggunaan data oleh pihak ketiga. Sementara itu, perlindungan represif diberikan melalui hak subjek data untuk memperoleh pemulihan, mengajukan gugatan dan memperoleh ganti rugi, serta melalui penerapan sanksi administratif dan pidana terhadap pelanggaran yang memenuhi ketentuan Undang-Undang Perlindungan Data Pribadi. Perlindungan hukum yang tersedia seharusnya tidak hanya mencegah penyalahgunaan, tetapi juga memberikan mekanisme pemulihan yang efektif ketika pelanggaran telah terjadi. Efektivitas perlindungan data pribadi nasabah pada akhirnya sangat bergantung pada kemampuan lembaga jasa keuangan untuk mengendalikan seluruh siklus pemrosesan data dan memastikan adanya pertanggungjawaban ketika pihak yang memperoleh akses menyalahgunakan data tersebut

**SARAN**

1. Diperlukan penguatan pengaturan dan pengawasan terhadap penyerahan serta pemrosesan data pribadi nasabah oleh pihak ketiga antara Otoritas Jasa Keuangan dengan lembaga jasa keuangan. Penggunaan pihak ketiga dalam penyelenggaraan layanan jasa keuangan perlu disertai pembatasan yang lebih jelas mengenai tujuan pemrosesan, jenis dan ruang lingkup data yang dapat diberikan, jangka waktu penggunaan, kewenangan pihak ketiga, serta kewajiban penghapusan atau pemusnahan data setelah tujuan pemrosesan berakhir. Lembaga jasa keuangan juga perlu memastikan adanya mekanisme pengawasan dan pencatatan akses

terhadap data sehingga dapat diketahui pihak yang mengakses, menggunakan, atau memindahkan data nasabah. Penguatan tersebut diperlukan agar penyerahan data kepada pihak ketiga tidak dipahami sebagai pengalihan kendali atas data pribadi, melainkan sebagai pemrosesan terbatas yang tetap berada dalam tanggung jawab lembaga jasa keuangan sebagai pihak yang menentukan tujuan pemrosesan.

2. Perlindungan represif terhadap nasabah perlu diperkuat melalui mekanisme pengaduan, penyelesaian sengketa, dan pemulihan kerugian yang lebih efektif. Nasabah yang mengalami penyalahgunaan data pribadi harus memperoleh akses yang mudah terhadap mekanisme pengaduan dan penyelesaian sengketa serta memperoleh kepastian mengenai pihak yang bertanggung jawab ketika pelanggaran dilakukan oleh pihak ketiga. Penerapan hak untuk menggugat dan memperoleh ganti rugi sebagaimana diatur dalam Undang-Undang Perlindungan Data Pribadi perlu didukung dengan mekanisme pembuktian dan penyelesaian sengketa yang tidak menempatkan seluruh beban pembuktian pada nasabah sebagai pemilik data. Selain pemulihan terhadap kerugian nasabah, pengenaan sanksi administratif maupun pidana perlu diterapkan secara proporsional terhadap pihak yang melakukan penyalahgunaan data. Langkah tersebut diperlukan agar perlindungan hukum tidak berhenti pada kewajiban preventif bagi penyelenggara jasa keuangan, tetapi benar-benar memberikan pemulihan terhadap hak nasabah ketika terjadi pelanggaran kerahasiaan dan penyalahgunaan data pribadi.

**UCAPAN TERIMA KASIH**

Terima kasih yang tiada terbilang untuk dosen pembimbing, semua dosen pemangku mata kuliah dan para staf Program Studi Magister Ilmu Hukum Pascasarjana Universitas Jayabaya serta semua pihak yang telah mebantu penyusunan jurnal Hukum ini.

**DAFTAR PUSTAKA**

Alan Westin, *Privacy And Freedom*, Ig Publishing, New York, 1967, hlm. 147

Danrivanto Budhijanto, *Hukum Pelindungan Data Pribadi di Indonesia*, Cyberlaw & Cybersecurity, Bandung: PT Refika Aditama, 2023

Edmon Makarim, *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik*, Jakarta: Rajawali Pers dan Lembaga Kajian Hukum Teknologi Fakultas Hukum Universitas Indonesia, 2010

Gliddheo Algifariyano Riyadi, *Kerahasiaan Data dalam Peraturan Perundang undangan Pelindungan Data Pribadi di Indonesia*, Center for Indonesian Policy Studies, 2021

Heather Leawoods, *Gustav Radbruch: An Extraordinary Legal Philosopher*, Wash. UJL & Pol'y 2, (2000)

Jan Michiel Otto, *Shaping the Rule of Law: Considerations from Indonesia* (The Hague: Van Vollenhoven Institute, Leiden University, 2003), hlm. 18–25

Jan Michiel Otto, *Shaping the Rule of Law: Considerations from Indonesia The Hague: Van Vollenhoven Institute*, Leiden University, 2003

KOMDIGI, *Kemkomdigi Tindak Delapan Aplikasi Diduga Menyalahgunakan Data Nasabah Pembiayaan,* https://www.komdigi.go.id/berita/siaran-pers/detail/kemkomdigi-tindak-delapan-aplikasi-diduga-menyalahgunakan-data-nasabah-pembiayaan [diakses pada 25/07/2026 pukul 14:21 WIB]

Muhammad, Abdul Kadir**,** *Hukum dan Penelitian Hukum*. Citra Aditya Bakti: Bandung, 2024

Nenny Rianarizkiwati, Kebebasan Informasi Versus Hak Atas Privasi Tanggung Jawab Negara Dalam Pelindungan Data Pribadi , Depok: Infermia Publishing, 2020

Olisias Gultom et.al, *Pelindungan Data Pribadi di Indonesia Menyikapi Liberalisasi Ekonomi Digital*, Indonesia For Global Justice, 2021

Otoritas Jasa Keuangan, *Laporan Kinerja OJK Triwulan II Tahun 2024*, Bab VIII mengenai layanan konsumen, yang menunjukkan bahwa penipuan (*phishing*, *skimming*, dan *social engineering*) merupakan salah satu jenis permasalahan yang banyak dilaporkan pada sektor perbankan, sedangkan perilaku petugas penagihan menjadi salah satu pengaduan dominan pada sektor IKNB

Otoritas Jasa Keuangan, *Laporan Kinerja OJK Triwulan II Tahun 2024*, Bab VIII. Laporan tersebut menunjukkan bahwa sengketa mengenai perilaku petugas penagihan serta *fraud* eksternal (penipuan, pembobolan rekening, *skimming*, dan *cyber crime*) termasuk dalam jenis sengketa yang dominan. Selain itu, Satgas PASTI menerima 3.306 pengaduan pada Triwulan II 2024, menghentikan 1.191 entitas pinjaman online ilegal, memblokir 185 rekening bank dan 801 nomor kontak pihak penagih yang terkait dengan aktivitas pinjaman online ilegal.

Phillipus M. Hadjon, *Pelindungan Hukum Bagi Rakyat di Indonesia,* Surabaya: PT Bina Ilmu, 1998

Phillipus M. Hadjon, *Pelindungan Hukum Bagi Rakyat Indonesia*, Surabaya, PT. Bina Ilmu, 1987

Phillipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat di Indonesia* (Surabaya: PT Bina Ilmu, 1987), hlm. 1–5.

Phillipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat Indonesia*, Surabaya, PT. Bina Ilmu, 1987, hlm. 25

Richardus Eko Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, Yogyakarta: Graha Ilmu, 2014

Rizky PP Karo-Karo dan Teguh Prasetya, *Pengaturan Pelindungan Data Pribadi di Indonesia*, Perspektif Teori Keadilan Bermartabat, Jakarta: Nusa Media, 2020

Satjipto Rahardjo, *Ilmu Hukum*, PT. Citra Aditya Bakti, Bandung, 2000

Sunarmi, *Pelindungan Data Pribadi Dalam Transaksi Elektronik di Indonesia dalam Revolusi Industri 4.0, Pembaharuan Hukum Nasional Indonesia di Era Industri 4.0 (Pokok-Pokok Pemikiran Guru Besar Ilmu Hukum) Jilid I*, Depok: PT RajaGrafindo Persada, 2021

Sunggono, Bambang, *Metode Penelitian Hukum*. Raja Grafindo Persada: Jakarta, 1996

Wignjosobroto, Soetandyo**,** *Hukum: Paradigma, Metode, dan Dinamika Masalah-Masalahnya*. Huma: Jakarta, 2002

**Peraturan Perundang-Undangan**

Undang-Undang Dasar Republik Indonesia Tahun 1945

Undang-Undang Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan;

Undang-Undang Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik;

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi;

Peraturan Otoritas Jasa Keuangan (POJK) Nomor 22 Tahun 2023 Tentang Pelindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE)